Available online at www.sciencedirect.com

SCIENCE DIRECT®

Applied Mathematics Letters 19 (2006) 340–344

Applied Mathematics Letters

www.elsevier.com/locate/aml

On the nonlinearity of linear recurrence sequences

Igor E. Shparlinski[a,*], Arne Winterhof[b]

[a] *Department of Computing, Macquarie University, Sydney, NSW 2109, Australia*
[b] *Johann Radon Institute for Computational and Applied Mathematics, Altenberger Straße 69, A-4040 Linz, Austria*

Received 29 March 2005; accepted 15 April 2005

Abstract

We obtain an upper bound on exponential sums of a new type with linear recurrence sequences. We apply this bound to estimate the Fourier coefficients, and thus the nonlinearity, of a Boolean function associated with a linear recurrence sequence in a natural way.

Keywords: Nonlinearity; Linear recurrence sequences; Fourier coefficients; Exponential sums

1. Introduction

Let p be a prime number and let $\mathbb{F}_p$ denote the finite field of p elements, which we identify with the set $\{0, 1, \ldots, p-1\}$.

Let $(s_k)_{k=0}^{\infty}$ be a linear recurrence sequence over $\mathbb{F}_p$ of order n, satisfying

$$s_{k+n} = c_{n-1}s_{k+n-1} + \cdots + c_0 s_k, \qquad k = 0, 1, \ldots,$$

with irreducible characteristic polynomial

$$F(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_0 \in \mathbb{F}_p[X].$$

It is known that any such sequence is periodic with least period $t \mid p^n - 1$; see Lemma 2 below.

For an integer $m \geq 1$ and a real z we write $\mathbf{e}_m(z) = \exp(2\pi \mathrm{i} z/m)$.

* Corresponding author. Tel.: +61 9850 9585; fax: +61 9850 9551.
E-mail addresses: igor@ics.mq.edu.au (I.E. Shparlinski), arne.winterhof@oeaw.ac.at (A. Winterhof).

0893-9659/$ - see front matter
doi:10.1016/j.aml.2005.04.015

There is a very long history of studying exponential sums

$$S(a) = \sum_{k=0}^{t-1} \mathbf{e}_p(s_k)\mathbf{e}_t(ak)$$

and, in particular, we recall the well known bound of [8]

$$\max_{a=0,\ldots,t-1} |S(a)| \le p^{n/2}; \tag{1}$$

see also [6, Theorem 5.1] or [7, Theorem 8.78]. The bound (1) and its various modifications have found an enormous number of applications in number theory and theory of pseudorandom numbers; see [6,7,10].

However, for applications of linear recurrence sequences to cryptography, and to stream ciphers in particular, bounds of different sums become more important.

We denote by $\mathcal{B}$ the set of n-digit integers to base p

$$\mathcal{B} = \{h \in \mathbb{Z} : 0 \le h \le p^n - 1\}.$$

Throughout the work we do not distinguish between n-digit integers $h \in \mathcal{B}$ and their p-ary expansions (we add extra leading zeros if necessary to make p-ary expansions of all $h \in \mathcal{B}$ of the same length n). Thus $\mathcal{B}$ can be considered as the n-dimensional cube $\mathcal{B} = \mathbb{F}_p^n$. In particular, for $h, r \in \mathcal{B}$, $\langle h, r\rangle$ denotes the inner product of h, r considered as n-dimensional p-ary vectors. That is,

$$\langle h, r\rangle = h_1r_1 + \cdots + h_nr_n$$

where

$$h = (h_1, \ldots, h_n) \qquad \text{and} \qquad r = (r_1, \ldots, r_n)$$

are p-ary digits of h and r.

That is, for $b \in \mathcal{B}$ we define the following sum

$$T(b) = \sum_{k=0}^{t-1} \mathbf{e}_p\left(s_k + \langle b, k\rangle\right).$$

In particular, we have $T(0) = S(0)$. In this work we prove the following bound on $T(b)$ for arbitrary $b \in \mathcal{B}$.

Theorem 1. *If the characteristic polynomial of the linear recurrence sequence $(s_k)_{k=0}^{\infty}$ is irreducible, then*

$$\max_{b\in\mathcal{B}} |T(b)| = O(t^{3/4}p^{n/8}n^{1/4}),$$

where the implied constant depends on p.

2. Auxiliary results

Here we collect two well known statements about linear recurrence sequences.

The first one is contained in [7, Theorems 8.28 and 8.29].

Lemma 2. *All nonzero linear recurrence sequences with the same irreducible characteristic polynomial of degree n over $\mathbb{F}_p$ are purely periodic with the same period t such that $t \mid p^n - 1$.*

We also need the following bound of exponential sums with linear recurrence sequences, which has been established in [8]; see also [6, Theorem 5.1] or [7, Theorem 8.81]. In fact this bound also follows from (1) by standard arguments.

Lemma 3. *For any nonzero linear recurrence sequences $(a_k)_{k=0}^{\infty}$ with irreducible characteristic polynomial of degree n over $\mathbb{F}_p$ and of period t, the bound*

$$\sum_{0 \le u < U} \mathbf{e}_p(a_u) = O\left(p^{n/2} \log t\right)$$

holds for all $1 \le U \le t$.

3. Proof of Theorem 1

We define the integer ν by the inequalities

$$p^{\nu} \le t^{1/2} p^{n/4} n^{1/2} < p^{\nu+1}$$

and write $d = (b_0, \ldots, b_{\nu-1})$ and $e = (b_{\nu}, \ldots, b_{n-1})$.

Every $k \in \mathcal{B}$ can be written in a unique way as $k = u + vp^{\nu}$ with integers u and v such that $0 \le u < p^{\nu}$ and $0 \le v < p^{n-\nu}$, and for such a representation we have

$$\langle b, k \rangle = \langle d, u \rangle + \langle e, v \rangle.$$

Let us put $V = \lfloor tp^{-\nu} \rfloor$. Therefore, we have

$$\begin{aligned} |T(b)| &= \left| \sum_{k=0}^{Vp^{\nu}-1} \mathbf{e}_p(s_k + \langle b, k \rangle) \right| + O(p^{\nu}) \\ &= \left| \sum_{u=0}^{p^{\nu}-1} \sum_{v=0}^{V-1} \mathbf{e}_p\left(s_{u+vp^{\nu}} + \langle d, u \rangle + \langle e, v \rangle\right) \right| + O(p^{\nu}) \\ &= \left| \sum_{u=0}^{p^{\nu}-1} \mathbf{e}_p(\langle d, u \rangle) \sum_{v=0}^{V-1} \mathbf{e}_p(s_{u+vp^{\nu}} + \langle e, v \rangle) \right| + O(p^{\nu}). \end{aligned}$$

Hence

$$|T(b)| \le W + O(p^{\nu}), \tag{2}$$

where

$$W = \sum_{u=0}^{p^{\nu}-1} \left| \sum_{v=0}^{V-1} \mathbf{e}_p(s_{u+vp^{\nu}} + \langle e, v \rangle) \right|.$$

By the Cauchy inequality we get

$$\begin{aligned} W^2 &\le p^{\nu} \sum_{u=0}^{p^{\nu}-1} \left| \sum_{v=0}^{V-1} \mathbf{e}_p(s_{u+vp^{\nu}} + \langle e, v \rangle) \right|^2 \\ &= p^{\nu} \sum_{u=0}^{p^{\nu}-1} \sum_{v,w=0}^{V-1} \mathbf{e}_p(s_{u+vp^{\nu}} + \langle e, v \rangle - s_{u+wp^{\nu}} - \langle e, w \rangle). \end{aligned}$$

Hence

$$W^2 \le p^\nu \sum_{v,w=0}^{V-1} \left| \sum_{u=0}^{p^\nu-1} \mathbf{e}_p(s_{u+vp^\nu} - s_{u+wp^\nu}) \right|. \tag{3}$$

It is clear that $(a_k)_{k=0}^\infty = (s_{k+vp^\nu} - s_{k+wp^\nu})_{k=0}^\infty$ is a linear recurrence sequence with the same irreducible characteristic polynomial as the original sequence $(s_k)_{k=0}^\infty$—it is either identical to zero or of the same least period t; see [7, Theorem 8.28].

Certainly $(a_k)_{k=0}^\infty$ is identical to zero if and only if

$$vp^\nu \equiv wp^\nu \pmod t. \tag{4}$$

By Lemma 2 we have $t \mid p^n - 1$; therefore $\gcd(t, p) = 1$. Thus (4) is possible only if $v \equiv w \pmod t$ and thus for only V pairs of $v, w \in \{0, \ldots, V-1\}$ (when $v = w$). In this case the inner sum in (3) is trivial and is equal to p^ν.

Therefore, if $v \not\equiv w \pmod t$, then we see that Lemma 3 applies to the corresponding inner sum in (3). Taking into account that $O(p^{n/2}\log t) = O(p^{n/2}n)$, we obtain

$$W^2 = O(p^\nu(Vp^\nu + V^2p^{n/2}n)) = O(tp^\nu + t^2p^{n/2-\nu}n),$$

which, with the above choice of ν, leads us to

$$W = O(t^{3/4}p^{n/8}n^{1/4}).$$

Since otherwise the theorem is trivial we may assume that $t > p^{n/2}n$ and the desired bound follows by (2). □

4. Applications

In particular, in the case of the most practical interest, where $p = 2$ and a binary linear recurrence sequence $(s_k)_{k=0}^\infty$ of the largest possible period $t = 2^n - 1$, the sums $T(b)$ are closely related to the properties of the following Boolean function:

$$f(k) = \begin{cases} s_k, & \text{if } 0 \le k \le 2^n - 2, \\ 1, & \text{if } k = 2^n - 1. \end{cases} \tag{5}$$

Let $\widehat{f}$ be the discrete Fourier transform of f, that is

$$\widehat{f}(b) = 2^{-n} \sum_{k \in \mathcal{B}} (-1)^{f(k)+\langle b,k\rangle}, \qquad b \in \mathcal{B}.$$

We recall that

$$N(f) = 2^{n-1} - 2^{n-1} \max_{b \in \mathcal{B}} |\widehat{f}(b)|$$

is called the *nonlinearity* of f; see [1–5,9,11] for the cryptographic significance of this notion. The nonlinearity of f gives the smallest possible Hamming distance between the vector of values of f and the vector of values of a linear function in n variables over $\mathbb{F}_2$, the field of two elements.

Clearly

$$\widehat{f}(b) = 2^{-n}(T(b) \pm 1).$$

Thus our result implies the bound

$$N(f) = 2^{n-1} + O(2^{7n/8} n^{1/4}) \tag{6}$$

on the nonlinearity of the Boolean function (5) in the case of the period $t = 2^n - 1$.

We remark that the bound (6) is not as strong as the best known bounds on specially designed Boolean functions; see [1–5,9,11] and references therein. However the purpose of this work is not to improve the current records on nonlinearity of the best known constructions, but rather to estimate this characteristic for Boolean functions naturally associated with linear recurrence sequences.

Acknowledgements

The authors would like to thank Sergei Agievich for bringing this question to their attention. During the preparation of this work, I.S. was supported in part by ARC grant DP0211459, A.W. was supported in part by the Austrian Academy of Sciences and by FWF grant S8313.

References

[1] C. Carlet, On cryptographic complexity of Boolean functions, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, 2002, pp. 53–69.
[2] C. Carlet, On the degree, nonlinearity, algebraic thickness, and nonnormality of Boolean functions, with developments on symmetric functions, IEEE Trans. Inform. Theory 50 (2004) 2178–2185.
[3] C. Carlet, C. Ding, Highly nonlinear mappings, J. Complexity 20 (2004) 205–244.
[4] C. Carlet, P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Finite Fields Appl. 8 (2002) 120–130.
[5] C. Carlet, Y. Tarannikov, Covering sequences of Boolean functions and their cryptographic significance, Des. Codes Cryptogr. 25 (2002) 263–279.
[6] G. Everest, A.J. van der Poorten, I.E. Shparlinski, T.B. Ward, Recurrence Sequences, Amer. Math. Soc., 2003.
[7] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[8] N.M. Korobov, The distribution of non-residues and of primitive roots in recurrence series, Dokl. Akad. Nauk SSSR 88 (1953) 603–606 (in Russian).
[9] P. Štanikă, Nonlinearity, local and global avalanche characteristics of balanced Boolean functions, Discrete Math. 248 (2002) 181–193.
[10] I.E. Shparlinski, Finite Fields: Theory and Computation, Kluwer Acad. Publ., Dordrecht, 1999.
[11] Y. Zheng, X.M. Zhang, Connections among nonlinearity, avalanche and correlation immunity, Theoret. Comp. Sci. 292 (2003) 697–710.